

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Reinhard SCHERTZ

On the generalized principal ideal theorem of complex multiplication

Tome 18, n° 3 (2006), p. 683-691.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_3_683_0>

© Université Bordeaux 1, 2006, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

On the generalized principal ideal theorem of complex multiplication

par REINHARD SCHERTZ

Dedicated to Michael Pohst on his 60th birthday

RÉSUMÉ. Dans le p^n -ième corps cyclotomique \mathbb{Q}_{p^n} , p un nombre premier, $n \in \mathbb{N}$, le premier p est totalement ramifié, l'idéal au dessus de p dans \mathbb{Q}_{p^n} étant engendré par $\omega_n = \zeta_{p^n} - 1$ avec une racine primitive p^n -ième de l'unité $\zeta_{p^n} = e^{\frac{2\pi i}{p^n}}$. De plus ces nombres constituent un ensemble qui vérifie la relation de norme $\mathbf{N}_{\mathbb{Q}_{p^{n+1}}/\mathbb{Q}_{p^n}}(\omega_{n+1}) = \omega_n$. Le but de cet article est d'établir un résultat analogue pour les corps de classes de rayon $K_{\mathfrak{p}^n}$ de conducteur \mathfrak{p}^n d'un corps quadratique imaginaire K , où \mathfrak{p}^n est une puissance d'un idéal premier dans K . Un tel résultat est obtenu en remplaçant la fonction exponentielle par une fonction elliptique convenable.

ABSTRACT. In the p^n -th cyclotomic field \mathbb{Q}_{p^n} , p a prime number, $n \in \mathbb{N}$, the prime p is totally ramified and the only ideal above p is generated by $\omega_n = \zeta_{p^n} - 1$, with the primitive p^n -th root of unity $\zeta_{p^n} = e^{\frac{2\pi i}{p^n}}$. Moreover these numbers represent a norm coherent set, i.e. $\mathbf{N}_{\mathbb{Q}_{p^{n+1}}/\mathbb{Q}_{p^n}}(\omega_{n+1}) = \omega_n$. It is the aim of this article to establish a similar result for the ray class field $K_{\mathfrak{p}^n}$ of conductor \mathfrak{p}^n over an imaginary quadratic number field K where \mathfrak{p}^n is the power of a prime ideal in K . Therefore the exponential function has to be replaced by a suitable elliptic function.

1. Introduction and results

Let K be an imaginary quadratic number field, \mathfrak{f} an integral ideal in K and $K_{\mathfrak{f}}$ the ray class field modulo \mathfrak{f} over K . In particular $K_{(1)}$ is the Hilbert class field of K . The generalized Principle Ideal Theorem [Sch2], [Sch3]¹ says that for any power of a prime ideal \mathfrak{p}^n there is an element $\pi_n \in K_{\mathfrak{p}^n}$

Manuscrit reçu le 22 novembre 2004.

¹In [Sch3] the following has to be corrected:

- 1) The prime ideal \mathfrak{q} in the definition of $H_{\mathfrak{q}}(z)$ must have the additional property $\gcd(\mathfrak{q}, \bar{\mathfrak{q}}) = 1$,
- 2) $H_{\mathfrak{q}}(1)$ has to be replaced by $H_{\mathfrak{q}}(\omega)$ with $\omega \equiv 1 \pmod{\mathfrak{q}}$, $\omega \equiv 0 \pmod{\bar{\mathfrak{q}}}$.

associated to $\mathfrak{p}^{\overline{[K_{p^n}:K(1)]}}$:

$$\pi_n \sim \mathfrak{p}^{\overline{[K_{p^n}:K(1)]}}.$$

The element π_n can be viewed as the elliptic analogue of the cyclotomic unit

$$\omega_n = e^{\frac{2\pi i}{p^n}} - 1$$

for the power p^n of a prime p . As an element of the p^n -th cyclotomic field \mathbb{Q}_{p^n} the element ω_n has the factorisation

$$\omega_n \sim (p)^{\overline{[\mathbb{Q}_{p^n}:\mathbb{Q}]}}.$$

Moreover ω_n has the following nice properties that can easily be verified:

- $\omega_n = e_n(1)$ with the p^n periodic function $e_n(z) = 1 - e^{\frac{2\pi i}{p^n}z}$.
- Let $\mathbb{C}_{p^n\mathbb{Z}}$ denote the field of p^n periodic meromorphic functions on \mathbb{C} , then we have the norm relation for $n \geq 0$

$$e_n(z) = N_{\mathbb{C}_{p^{n+1}\mathbb{Z}}/\mathbb{C}_{p^n\mathbb{Z}}}(e_{n+1}(z)) = \prod_{\xi \in p^n\mathbb{Z} \bmod p^{n+1}\mathbb{Z}} e_{n+1}(z + \xi).$$

- For $z = 1$ the last relation becomes a norm relation between number fields, if $n \geq 1$:

$$\omega_n = N_{\mathbb{Q}_{p^{n+1}}/\mathbb{Q}_{p^n}}(\omega_{n+1}) = \prod_{\xi \in p^n\mathbb{Z} \bmod p^{n+1}\mathbb{Z}} e_{n+1}(1 + \xi)$$

- and

$$\left. \frac{e_0(z)}{e_1(z-1)} \right|_{z=1} = p.$$

It is the aim of this article to give a construction of π_n having the same nice properties. For a complex lattice Γ we therefore consider the Klein normalization of the Weierstrass σ -function

$$\varphi(z|\Gamma) = e^{-\frac{zz^*}{2}} \sigma(z|\Gamma) \sqrt[12]{\Delta(\Gamma)},$$

where $\Delta(\Gamma)$ is the discriminant of the theory of elliptic functions. Herein z^* is defined for a complex number z by

$$z^* = z_1\omega_1^* + z_2\omega_2^*,$$

with the real coordinates z_1, z_2 from the representation $z = z_1\omega_1 + z_2\omega_2$ by a basis ω_1, ω_2 of Γ and the quasiperiods $\omega_i^* = 2\zeta(\frac{\omega_i}{2}|\Gamma)$ of the Weierstrass ζ -function. The first factor $e^{-\frac{zz^*}{2}} \sigma(z|\Gamma)$ in the definition of $\varphi(z|\Gamma)$ is clearly independent of the choice of basis ω_1, ω_2 of Γ . To fix the 12-th root $\sqrt[12]{\Delta(\Gamma)}$ we use the identity

$$\Delta(\Gamma) = \left(\frac{2\pi i}{\omega_2}\right)^{12} \eta\left(\frac{\omega_1}{\omega_2}\right)^{24}$$

for a basis of Γ oriented by $\Im\left(\frac{\omega_1}{\omega_2}\right) > 0$ and set

$$\sqrt[12]{\Delta(\Gamma)} = \left(\frac{2\pi i}{\omega_2}\right) \eta\left(\frac{\omega_1}{\omega_2}\right)^2.$$

So the value $\varphi(z|\Gamma)$ is only well defined up to a 12-th root of unity depending on the basis chosen for its definition. However products where all the $\sqrt[12]{\Delta(\Gamma)}$ -factors cancel out are independent of the choice of basis choosing the same basis for each factor.

We fix an arbitrary prime ideal \mathfrak{p} in K and an integral auxiliary ideal $\mathfrak{q} \nmid 2$ that is prime to \mathfrak{p} and satisfies

$$\gcd(\mathfrak{q}, \bar{\mathfrak{q}}) = 1.$$

For $n \in \mathbb{N}$ we define

$$E_n(z) := \frac{\varphi(z - \gamma_n | \mathfrak{qp}^n) \varphi(z + \gamma_n | \mathfrak{qp}^n)}{\varphi^2(z | \mathfrak{qp}^n)}$$

with a solution γ_n of the congruences

$$\begin{aligned} \gamma_n &\equiv 0 \pmod{\mathfrak{p}^n}, \\ \gamma_n &\equiv 1 \pmod{\mathfrak{q}}, \\ \gamma_n &\equiv 0 \pmod{\bar{\mathfrak{q}}}. \end{aligned}$$

Note that $E_n(z)$ is well defined because all Δ -factors are canceling out if we choose the same basis of \mathfrak{qp}^n for every φ -value. Using the identity $\wp(u) - \wp(v) = -\frac{\sigma(u-v)\sigma(u+v)}{\sigma^2(u)\sigma^2(v)}$, we can express E_n by the Weierstrass \wp -function:

$$E_n(z) = -\varphi^2(\gamma_n | \mathfrak{qp}^n) \left(\frac{\wp(z | \mathfrak{qp}^n)}{\sqrt[6]{\Delta(\mathfrak{qp}^n)}} - \frac{\wp(\gamma_n | \mathfrak{qp}^n)}{\sqrt[6]{\Delta(\mathfrak{qp}^n)}} \right)$$

and we can conclude that E_n is elliptic with respect to the lattice \mathfrak{qp}^n . Moreover E_n satisfies the following norm relation:

Theorem 1. *Let $\mathbb{C}_{\mathfrak{qp}^n}$ denote the field of elliptic functions with respect to \mathfrak{qp}^n , $n \geq 0$. Then $\mathbb{C}_{\mathfrak{qp}^{n+1}}/\mathbb{C}_{\mathfrak{qp}^n}$ is a Galois extension, the Galois group consisting of all substitutions*

$$g(z) \mapsto g(z + \xi), \quad \xi \in \mathfrak{qp}^n \pmod{\mathfrak{qp}^{n+1}}$$

for $g \in \mathbb{C}_{\mathfrak{qp}^{n+1}}$ and we have the norm relation

$$E_n(z) = \mathbf{N}_{\mathbb{C}_{\mathfrak{qp}^{n+1}}/\mathbb{C}_{\mathfrak{qp}^n}}(E_{n+1}(z)) = \prod_{\xi \in \mathfrak{qp}^n \pmod{\mathfrak{qp}^{n+1}}} E_{n+1}(z + \xi).$$

For the singular values $E_n(1)$ we obtain:

Theorem 2. *Let \mathfrak{p} and \mathfrak{q} be as above and let Φ denote the Euler function in K . Then*

- (1) $E_n(1) \in K_{\mathfrak{q}\mathfrak{p}^n}$ for $n \geq 0$,
- (2) $E_n(1) \sim \mathfrak{p}^{\frac{1}{\Phi(\mathfrak{p}^n)}}$ for $n \geq 1$,
- (3) $E_n(1) = \mathbf{N}_{K_{\mathfrak{q}\mathfrak{p}^{n+1}}/K_{\mathfrak{q}\mathfrak{p}^n}}(E_{n+1}(1)) = \prod_{\xi \in \mathfrak{q}\mathfrak{p}^n \bmod \mathfrak{q}\mathfrak{p}^{n+1}} E_{n+1}(1 + \xi)$ for $n \geq 1$,
- (4) $\left. \frac{E_0(z)}{E_1(z-1+\gamma_1)} \right|_{z=1} = \mathbf{N}_{K_{\mathfrak{q}\mathfrak{p}}/K_{\mathfrak{q}}}(E_1(1)) = \frac{\varphi(1+\gamma_1|\mathfrak{q})\varphi(\gamma_1|\mathfrak{q}\mathfrak{p})^2}{\varphi(2\gamma_1|\mathfrak{q}\mathfrak{p})\varphi(1|\mathfrak{q})^2} \sqrt[12]{\frac{\Delta(\mathfrak{q})}{\Delta(\mathfrak{q}\mathfrak{p})}} \sim \mathfrak{p}$.

To obtain the analogous result for the extension $K_{\mathfrak{p}^{n+1}}/K_{\mathfrak{p}^n}$ that we were aiming at, we have to get rid of the auxiliary ideal \mathfrak{q} . Therefore we need the following (well known)

Lemma. *For any integral ideal \mathfrak{a} in K*

$$\gcd\{N(\mathfrak{q}) - 1 \mid \mathfrak{q} \text{ prime ideal in } K, \mathfrak{q} \nmid 2\bar{\mathfrak{q}} \mathfrak{a}\} = w_K,$$

where w_K denotes the number of roots of unity in K .

So we can choose finitely many prime ideals \mathfrak{q}_i , $i = 1, \dots, s$ of degree 1 that are prime to $N(\mathfrak{p})$ and integers $x_i \in \mathbb{Z}$ so that

$$x_1(N(\mathfrak{q}_1) - 1) + \dots + x_s(N(\mathfrak{q}_s) - 1) = w_K.$$

For each \mathfrak{q}_i we define a set of functions $E_{n,i}(z)$ as above with parameters $\gamma_{n,i}$. Taking relative norms we obtain

$$\mathbf{N}_{K_{\mathfrak{q}_i\mathfrak{p}^n}/K_{\mathfrak{p}^n}}(E_{n,i}(1)) \sim \mathfrak{p}^{\frac{N(\mathfrak{q}_i)-1}{\Phi(\mathfrak{p}^n)}}$$

for $n \geq 1$. Hence

$$\pi_n := \prod_{i=1}^s \left(\mathbf{N}_{K_{\mathfrak{q}_i\mathfrak{p}^n}/K_{\mathfrak{p}^n}}(E_{n,i}(1)) \right)^{x_i}$$

is an element in $K_{\mathfrak{p}^n}$ having the factorisation

$$\pi_n \sim \mathfrak{p}^{\frac{w_K}{\Phi(\mathfrak{p}^n)}}.$$

This is what we were aiming at because

$$[K_{\mathfrak{p}^n} : K_{(1)}] = \frac{w(\mathfrak{p}^n)}{w_K} \Phi(\mathfrak{p}^n),$$

where $w(\mathfrak{p}^n)$ denotes the number of roots of unity in K that are congruent to 1 mod \mathfrak{p}^n . This implies

$$\pi_n \sim \mathfrak{p}^{\frac{w(\mathfrak{p}^n)}{[K_{\mathfrak{p}^n}:K_{(1)}]}}$$

where

$$w(\mathfrak{p}^n) = 1$$

except for the cases

- (i) $\mathfrak{p} \mid 2, n \leq 2$, where $w(\mathfrak{p}^n) \in \{1, 2\}$, if $d_K \neq -4$ and $w(\mathfrak{p}^n) \in \{1, 2, 4\}$ if $d_K = -4$;
- (ii) $\mathfrak{p} \mid 3, n = 1, d_K = -3$, where $w(\mathfrak{p}^n) = 2$.

Moreover we will show now that this element can be written analogously to the cyclotomic case. We therefore observe that by reciprocity law the conjugates of the singular values $E_{n,i}(1)$ over $K_{\mathfrak{p}^n}$ are given by

$$E_{n,i}(1)^{\sigma(\lambda)} = \frac{\varphi(\lambda - \gamma_{n,i}\lambda \mid \mathfrak{q}_i \mathfrak{p}^n) \varphi(\lambda + \gamma_{n,i}\lambda \mid \mathfrak{q}_i \mathfrak{p}^n)}{\varphi^2(\lambda \mid \mathfrak{q}_i \mathfrak{p}^n)},$$

where $\sigma(\lambda)$ denotes the Frobenius automorphism of $K_{\mathfrak{q}\mathfrak{p}^n}/K_{\mathfrak{p}^n}$ of the ideal $(\lambda), \lambda \equiv 1 \pmod{\mathfrak{p}^n}$. So we define the function

$$E_n^*(z) := \prod_{i=1}^s \prod_{j=1}^{N(\mathfrak{q}_i)-1} \left(\frac{\varphi\left(z + (\lambda_{i,j}^{(n)} - 1) - \gamma_{n,i}\lambda_{i,j}^{(n)} \mid \mathfrak{q}_i \mathfrak{p}^n\right) \varphi\left(z + (\lambda_{i,j}^{(n)} - 1) + \gamma_{n,i}\lambda_{i,j}^{(n)} \mid \mathfrak{q}_i \mathfrak{p}^n\right)}{\varphi^2\left(z + (\lambda_{i,j}^{(n)} - 1) \mid \mathfrak{q}_i \mathfrak{p}^n\right)} \right)^{x_i}$$

where for fixed i and n the numbers

$$\lambda_{i,j}^{(n)}, j = 1, \dots, N(\mathfrak{q}_i) - 1$$

are a complete system of prime residue classen mod \mathfrak{q}_i satisfying

$$\lambda_{i,j}^{(n)} \equiv 1 \pmod{\mathfrak{p}^n}.$$

Herewith we can prove the following two Theorems:

Theorem 3. *Let \mathfrak{p} and $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ with \mathfrak{q}_i as above. Then the functions $E_n^*(z)$ are in $\mathbb{C}_{\mathfrak{q}\mathfrak{p}^n}$ for $n \geq 0$ and satisfy the Normrelation*

$$E_n^*(z) = \mathbf{N}_{\mathbb{C}_{\mathfrak{q}\mathfrak{p}^{n+1}}/\mathbb{C}_{\mathfrak{q}\mathfrak{p}^n}}(E_{n+1}^*(z)) = \prod_{\xi \in \mathfrak{q}\mathfrak{p}^n \pmod{\mathfrak{q}\mathfrak{p}^{n+1}}} E_{n+1}^*(z + \xi).$$

Theorem 4. *Let \mathfrak{p} and $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ with \mathfrak{q}_i as above and let Φ denote the Euler function in K . Then*

- (1) $E_n^*(1) \in K_{\mathfrak{p}^n}$ for $n \geq 0$,
- (2) $E_n^*(1) \sim \mathfrak{p}^{\overline{[K_{\mathfrak{p}^n}:K(1)]} \frac{w(\mathfrak{p}^n)}{w(\mathfrak{p}^n)}}$ for $n \geq 1$,
- (3) $E_n^*(1) = \mathbf{N}_{K_{\mathfrak{p}^{n+1}}/K_{\mathfrak{p}^n}}(E_{n+1}^*(1))^{\frac{w(\mathfrak{p}^n)}{w(\mathfrak{p}^{n+1})}} = \prod_{\substack{\xi \in \mathfrak{q}\mathfrak{p}^n \\ \pmod{\mathfrak{q}\mathfrak{p}^{n+1}}} E_{n+1}^*(1 + \xi)$ for $n \geq 1$,
- (4) $\mathbf{N}_{K_{\mathfrak{p}^n}/K(1)}(E_n^*(1)) \sim \mathfrak{p}^{w(\mathfrak{p}^n)}$.

Remark: The constructions of the above theorems can clearly be generalized to any integral ideal \mathfrak{a} prime to \mathfrak{q} instead of \mathfrak{p}^n with obvious norm relations for two ideals $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{a} \mid \mathfrak{b}$. Of course for a composite ideal \mathfrak{a} the singular values will be units.

2. Proofs

Proposition. *Let $\Gamma = [\omega, 1]$, $\hat{\Gamma} = [\frac{\omega}{n_1}, \frac{1}{n_2}]$ be complex lattices, $\Im(\omega) > 0$, $n_1, n_2 \in \mathbb{N}$. We consider the following system of representatives for $\hat{\Gamma}/\Gamma$:*

$$\xi = \frac{x\omega}{n_1} + \frac{y}{n_2}, \quad x = 0, \dots, n_1 - 1, \quad y = 0, \dots, n_2 - 1.$$

Expressing Δ by the η -function, $\Delta = (2\pi i)^{12}\eta^{24}$, we define the 12-th roots of $\Delta(\Gamma)$ and $\Delta(\hat{\Gamma})$ by

$$\sqrt[12]{\Delta(\Gamma)} := (2\pi i)\eta(\omega)^2, \quad \sqrt[12]{\Delta(\hat{\Gamma})} := (2\pi i)\eta(\frac{n_1\omega}{n_2})^2 n_2$$

and we set

$$l_\Gamma(z, \xi) = 2\pi i(z_1\xi_2 - z_2\xi_1).$$

Then

$$\prod_{\xi} e^{-\frac{1}{2}l_\Gamma(z, \xi)} \varphi(z + \xi|\Gamma) = \zeta \varphi(z|\hat{\Gamma})$$

with

$$\zeta = -\zeta_4^{n_1 n_2 + n_1} \zeta_8^{(n_1 - 1)(n_2 - 1)}$$

($\zeta_n := e^{\frac{2\pi i}{n}}$). Furthermore, dividing both sides of the product formula by $\varphi(z|\Gamma)$, the limit for $z \rightarrow 0$ yields

$$\prod_{\xi \neq 0} \varphi(\xi|\Gamma) = \zeta \frac{\sqrt[12]{\Delta(\hat{\Gamma})}}{\sqrt[12]{\Delta(\Gamma)}}.$$

Proof. The assertion of the Proposition is obtained by multiplying the q -expansions of the functions involved. Using the notations

$$Q_w = e^{2\pi iw}, \quad Q_{\frac{1}{w}} = e^{\pi iw}, \quad q = Q_\omega, \quad \hat{q} = Q_{\frac{n_2\omega}{n_1}}$$

the q -expansions of $\varphi(w|\Gamma)$ and $\varphi(z|\hat{\Gamma})$ are given by

$$\begin{aligned} \varphi(z + \xi|\Gamma) &= Q_{z+\xi}^{\frac{1}{2}(z_1+\xi_1)} (Q_{z+\xi}^{\frac{1}{2}} - Q_{z+\xi}^{-\frac{1}{2}}) q^{\frac{1}{12}} \prod_{n=1}^{\infty} (1 - q^n Q_{z+\xi})(1 - q^n Q_{z+\xi}^{-1}), \\ \varphi(z|\hat{\Gamma}) &= Q_{\frac{1}{n_2 z}}^{\frac{1}{2}n_1 z_1} (Q_{\frac{1}{n_2 z}}^{\frac{1}{2}} - Q_{\frac{1}{n_2 z}}^{-\frac{1}{2}}) \hat{q}^{\frac{1}{12}} \prod_{n=1}^{\infty} (1 - \hat{q}^n Q_{n_2 z})(1 - \hat{q}^n Q_{n_2 z}^{-1}). \end{aligned}$$

So the product in the Proposition is of the form

$$\prod_{\xi} e^{-\frac{1}{2}l_\Gamma(z, \xi)} \varphi(z + \xi|\Gamma) = f_1 f_2 f_3$$

with

$$\begin{aligned}
 f_1 &= e^{\frac{2\pi i}{2} \sum_{x,y} (z+\xi)(z_1+\xi_1) - z_1\xi_2 + z_2\xi_1}, \\
 f_2 &= \prod_{x,y} q^{\frac{1}{12}} (Q_{z+\xi}^{\frac{1}{2}} - Q_{z+\xi}^{-\frac{1}{2}}), \\
 f_3 &= \prod_{n=1}^{\infty} \prod_{x,y} (1 - q^n Q_{z+\xi})(1 - q^n Q_{z+\xi}^{-1}).
 \end{aligned}$$

Using the formulas $\sum_{k=1}^{m-1} k = \frac{m(m-1)}{2}$ and $\sum_{k=1}^{m-1} k^2 = \frac{m(m-1)(2m-1)}{6}$ we then obtain

$$f_1 = \zeta_8^{(n_1-1)(n_2-1)} Q_{n_2 z}^{\frac{n_1 z_1}{2}} Q_{n_2 z}^{\frac{n_1-1}{2}} \hat{q}^{\frac{(n_1-1)(2n_1-1)}{12}}, \quad \hat{q} = q^{\frac{n_1}{n_2}}.$$

Further, using the identity $\prod_{y=0}^{n_2-1} (a - b\zeta_{n_2}^y) = a^{n_2} - b^{n_2}$ we can write f_2 in the form

$$f_2 = -\zeta_4^{n_1 n_2 + n_1} Q_{n_2 z}^{-\frac{n_1-1}{2}} \hat{q}^{n_1 n_2 - \frac{n_1(n_1-1)}{4}} \prod_{x=1}^{n_1-1} (1 - \hat{q}^x Q_{n_2 z})$$

and in the same way

$$f_3 = \left(\prod_{k=n_1}^{\infty} (1 - \hat{q}^k Q_{n_2 z}) \right) \left(\prod_{k=1}^{\infty} (1 - \hat{q}^k Q_{n_2 z}^{-1}) \right).$$

Now, putting together the identities for f_1, f_2, f_3 we can easily derive our assertion. □

Proof of Theorem 1. First we observe that the assertion of the Proposition is also valid for arbitrary lattices $\Gamma \subset \hat{\Gamma}$, arbitrary systems $\{\xi\}$ of representatives and other normalization of the 12-th root of Δ , with possibly another constant ζ . This follows from the homogeneity and the transformation formula of the φ -function:

$$\varphi(\lambda z | \lambda \Gamma) = \varphi(z | \Gamma),$$

$$\varphi(z + \tau | \Gamma) = \psi(\tau) e^{\frac{1}{2}l_{\Gamma}(\tau, z)} \varphi(z | \Gamma) \text{ for } \tau \in \Gamma$$

with

$$\psi(\tau) = \begin{cases} 1, & \text{if } \tau \in 2\Gamma, \\ -1, & \text{if } \tau \in \Gamma \setminus 2\Gamma. \end{cases}$$

Considering the fact that $l_\Gamma(z, \xi)$ is linear in z we obtain from the generalized version of the Proposition just explained:

$$\prod_{\xi \in \mathfrak{qp}^n \bmod \mathfrak{qp}^{n+1}} E_{n+1}(z + \xi) = \frac{\varphi(z - \gamma_{n+1} | \mathfrak{qp}^n) \varphi(z + \gamma_{n+1} | \mathfrak{qp}^n)}{\varphi^2(z | \mathfrak{qp}^n)}.$$

Herein on the right γ_{n+1} can be replaced by γ_n using the transformation law of φ , because $\gamma_{n+1} \equiv \gamma_n \bmod \mathfrak{qp}^n$. This proves the formula of Theorem 1. □

Proof of Theorem 2. By reciprocity law of complex multiplication we know

$$\varphi(\delta | \mathfrak{qp}^n) \in K_{12N(\mathfrak{qp}^n)^2} \text{ for } \delta \in \mathfrak{D}_K$$

for every choice of basis in \mathfrak{qp}^n . Further, as can be found in [B-Sch], the action of a Frobenius automorphism $\sigma(\lambda)$ of $K_{12N(\mathfrak{qp}^n)^2}$ belonging to an integral principal ideal (λ) of \mathfrak{D}_K prime to $12N(\mathfrak{qp}^n)$ is of the form

$$\varphi(\delta | \mathfrak{qp}^n)^{\sigma(\lambda)} = \epsilon \varphi(\delta \lambda | \mathfrak{qp}^n)$$

with a root of unity ϵ independent of δ . This implies

$$E_n(\delta) \in K_{12N(\mathfrak{qp}^n)^2}$$

and

$$E_n(\delta)^{\sigma(\lambda)} = \frac{\varphi(\delta \lambda - \gamma_n \lambda | \mathfrak{qp}^n) \varphi(\delta \lambda + \gamma_n \lambda | \mathfrak{qp}^n)}{\varphi^2(\delta \lambda | \mathfrak{qp}^n)} \text{ for } \delta \in \mathfrak{D}_K \setminus \{0\}$$

with λ having the above properties. For $\lambda = 1 + \tau$, $\tau \in \mathfrak{qp}^n$, the φ -values in the numerator on the right side can be simplified by the transformation law of φ :

$$\begin{aligned} \varphi(\delta \lambda \pm \gamma_n \lambda | \mathfrak{qp}^n) &= \varphi(\delta \lambda \pm \gamma_n \pm \gamma_n \tau | \mathfrak{qp}^n) \\ &= \psi(\tau \gamma_n) e^{\frac{1}{2}l(\delta \lambda \pm \gamma_n, \pm \gamma_n \tau)} \varphi(\delta \lambda \pm \gamma_n | \mathfrak{qp}^n) \end{aligned}$$

with $l = l_{\mathfrak{qp}^n}$. So

$$E_n(\delta)^{\sigma(\lambda)} = e^{l(\gamma_n, \gamma_n \tau)} E_n(\delta \lambda).$$

Herein, using the rule $l(a, bc) = l(a\bar{b}, c)$,

$$l(\gamma_n, \gamma_n \tau) = l(\gamma_n \bar{\gamma}_n, \tau) \in 2\pi i\mathbb{Z}$$

because $\gamma_n \bar{\gamma}_n, \tau \in \mathfrak{qp}^n$, whence

$$E_n(\delta)^{\sigma(\lambda)} = E_n(\delta \lambda).$$

Now, considering the fact that E_n is elliptic with respect to \mathfrak{qp}^n , it follows

$$E_n(1)^{\sigma(\lambda)} = E_n(1) \text{ for } \lambda \equiv 1 \bmod \mathfrak{qp}^n$$

and we can conclude that $E_n(1)$ is in $K_{\mathfrak{qp}^n}$, because

$$\text{Gal}(K_{12N(\mathfrak{qp}^n)^2}/K_{\mathfrak{qp}^n}) = \{\sigma(\lambda) \mid \lambda \equiv 1 \bmod \mathfrak{qp}^n \text{ and prime to } N(\mathfrak{qp})\}.$$

The third assertion of Theorem 2 is obtained similarly: We have

$$\text{Gal}(K_{\mathfrak{qp}^{n+1}}/K_{\mathfrak{qp}^n}) = \{\sigma(1 + \xi) \mid \xi \in \mathfrak{qp}^n \bmod \mathfrak{qp}^{n+1}\}$$

and

$$E_{n+1}(1)^{\sigma(1+\xi)} = e^{l(\gamma_{n+1}\overline{\gamma_{n+1}}, \xi)} E_{n+1}(1 + \xi)$$

with $l = l_{\mathfrak{qp}^{n+1}}$, where of course $\sigma(1 + \xi)$ denotes the Frobenius automorphism of $K_{\mathfrak{qp}^{n+1}}$ belonging to $(1 + \xi)$. Again herein $l(\gamma_{n+1}\overline{\gamma_{n+1}}, \xi)$ is in $2\pi i\mathbb{Z}$ because $\xi \in \mathfrak{qp}^n$ and because $\gamma_{n+1}\overline{\gamma_{n+1}}$ is even in $\mathfrak{qp}^{n+1}\overline{\mathfrak{p}^{n+1}}$, whence

$$E_{n+1}(1)^{\sigma(1+\xi)} = E_{n+1}(1 + \xi),$$

which proves the third assertion.

Finally, the second assertion of Theorem 2 follows from the factorisation of the singular φ -values [Sch1]:

$$\varphi(\delta|\mathfrak{qp}^n) \sim \begin{cases} 1, & \text{if } o(\delta, \mathfrak{qp}^n) \text{ is composite,} \\ \mathfrak{p}^{\frac{1}{\Phi(\mathfrak{p}^r)}}, & \text{if } o(\delta, \mathfrak{qp}^n) = \mathfrak{p}^r, r \in \mathbb{N} \end{cases}$$

for every choice of basis in \mathfrak{qp}^n . Herein $\delta \in K \setminus \{0\}$ and $o(\delta, \mathfrak{qp}^n)$ denotes the denominator of the ideal $\frac{\delta}{\mathfrak{qp}^n}$. This factorisation implies that the first φ factor in the numerator of the definition of $E_n(1)$ has the factorisation $\mathfrak{p}^{\frac{1}{\Phi(\mathfrak{p}^n)}}$, whereas the other φ values are units. □

Proof of Theorem 3 and 4. The proof of Theorem 3 is completely analogous to the proof of Theorem 1. The first and second assertion of Theorem 4 have already been explained. The third assertion can easily be proved using the same arguments as in the proof of Theorem 2. □

References

[B-Sch] S. BETTNER, R. SCHERTZ, *Lower powers of elliptic units*. Journal de Théorie des Nombres de Bordeaux **13** (2001), 339–351.
 [Sch1] R. SCHERTZ, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*. J. Reine Angew. Math. **398** (1989), 105–129.
 [Sch2] R. SCHERTZ, *Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper*. Journal of Number Theory, Vol. **34** No. 1 (1990).
 [Sch3] R. SCHERTZ, *An Elliptic Resolvent*. Journal of Number Theory, Vol. **77** (1999), 97–121.

Reinhard SCHERTZ
 Institut für Mathematik der Universität Augsburg
 Universitätsstraße 8
 86159 Augsburg, Germany
E-mail: Reinhard.Schertz@Math.Uni-Augsburg.DE